PROXIOS

Proxios Security Posture

Three Layers of Security

Proxios' security posture is based upon a multi-layer approach to achieve end-to-end protection from threats. Using state-of-the-art processes, equipment, policies, and technologies, we have created a very high level of security while still allowing full application availability and a productive user experience. By leveraging our relationships with some of the most advanced industry leaders, like Dell SecureWorks, Palo Alto Networks, Cisco, Microsoft, and many others, Proxios remains at the forefront of data protection and security.

First Layer: Securing the Network

The first layer of our security posture involves securing the network using Application Aware (Layer 7) firewalls, both at the network perimeter, as well as between internal networks. Combined with IEEE 802.1q VLAN tagging, internal firewalls provide complete customer network isolation and protection. These firewalls also use secure, isolated execution areas to detect and stop incoming viruses and worms, blocking potential "zero day" infections. In addition, we run regular, internal and external penetration tests and vulnerability scans to ensure that all accesses are fortified.

Second Layer: Patch Management, Anti-virus, and Template Controls

Our second set of enforcement measures involves patch management, anti-virus programs, and template controls. By using enterprise class management of all server configurations, patching schedules, and anti-virus/anti-malware programs, Proxios ensures that each system is protected to the greatest degree against all known malware, as well as blocking as many potential infection points as possible. Patch management also makes certain that known problems in all the major software packages are closed as quickly as possible after a vendor releases the patch.

Final Layer: The Human Factor

The "human factor" is the final and most important layer of the posture. Aggressive change management policies are in place to prevent any potential problems, outages, or infections from unanticipated consequences that might result from system changes. As part of the protocol, Proxios employees receive extensive training on security matters, including email safety, web safety, and especially social engineering attempts. This shields the most vulnerable point of the operation: the human behind the keyboard.

In a modern enterprise, security must be a multi-layered effort. It is no longer acceptable to just have a firewall at the Internet access point and consider it secure. By using many different, complimentary technologies, Proxios ensures that all data entrusted to it is as secure as possible. The combination of comprehensive training, excellent management of the systems themselves, and a modern secure infrastructure design distinguishes Proxios at the leading edge of information security.

For more information, visit: www.proxios.com